(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 199 29 164 A 1**

(51) Int. Cl.[7]:
G 07 F 7/10
G 06 F 3/08

(21) Aktenzeichen: 199 29 164.0
(22) Anmeldetag: 25. 6. 1999
(43) Offenlegungstag: 11. 1. 2001

(71) Anmelder:
Giesecke & Devrient GmbH, 81677 München, DE

(72) Erfinder:
Merck, Martin, Dr., 81677 München, DE; Kolbeck, Alexander, 82362 Weilheim, DE; Stocker, Thomas, 81673 München, DE; Frey, Thomas, 85560 Ebersberg, DE; Weiß, Dieter, 81677 München, DE

(56) Entgegenhaltungen:
DE 197 18 115 A1
WO 98 09 257 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zum Betreiben eines zur Ausführung von nachladbaren Funktionsprogrammen ausgebildeten Datenträgers

(57) Vorgeschlagen wird ein Verfahren zum Betreiben eines zur Ausführung von nachladbaren Funktionsprogrammen ausgebildeten tragbaren Datenträgers. Verfahrensgemäß wird dabei auf dem Datenträger zunächst eine Laderschnittstelle installiert, welche das Nachladen von Ladeapplikationen gestattet, die ihrerseits dann das Laden von Funktionsprogrammen ermöglichen. Jeder Ladeapplikation wird ein nicht veränderbarer Verfügungsadreßraum zugeteilt. Vorgeschlagen wird weiter ein Verfahren zur Verwaltung eines zugeteilten Verfügungsadreßraumes. Zu nachzuladenen Anwendungsprogrammen werden danach Ausweise erstellt, welche eine Information über die Größe des für das Anwendungsprogramm benötigten Speicherplatzes enthalten. Entsprechend der auf den Ausweisen angelegten Größeninformation wird nachzuladenen Anwendungsprogrammen Adreßraum in der Speichereinrichtung zugeteilt. Weiterhin werden zu den Verfahren entsprechende Datenträger offenbart.

DE 199 29 164 A 1

DE 199 29 164 A 1

Beschreibung

Die Erfindung geht aus von einem Verfahren nach der Gattung des Hauptanspruchs.

Datenträger in Form von Chipkarten werden in einer zunehmenden Vielfalt von Anwendungsbereichen eingesetzt. Besonders verbreitet sind Karten gemäß der Norm ISO 7810, die aus einem Kunststoffträger bestehen, in den eine integrierte Halbleiterschaltung sowie Kontaktmittel zum Herstellen elektrischer Verbindungen mit einem entsprechenden Lesegerät eingebracht sind. Vorgeschlagen wurde auch, den Kartenträger zu verkleinern oder ganz fortzulassen, und stattdessen beispielsweise ein Einchip-Mikrocontroller in Armbanduhren, Schmuckstücke, Kleidungsstücke oder andere Gebrauchsgegenstände einzubauen. Der Begriff "Chipkarte" soll sich daher auf alle derzeitigen und zukünftigen transportablen(Klein-)Gegenstände erstrecken, in welche ein Mikrocontroller eingebettet ist, um es ihrem Besitzer oder Inhaber zu ermöglichen, chipkartentypische Interaktionen mit entsprechenden dafür vorgesehenen Interaktionsstationen vorzunehmen. Typische Chipkartenanwendungen sind die Kreditkarte, die Geldkarte, die Krankenversicherungskarte oder die Telefonkarte. Unter "Anwendung" wird dabei die Gesamtheit aller Daten, Befehle, Abläufe, Zustände, Mechanismen und Algorithmen innerhalb einer Chipkarte verstanden, die erforderlich sind, um eine Chipkarte im Rahmen eines Systems, beispielsweise eines Kreditkartenzahlungssystem, zu betreiben.

Üblicherweise entspricht jeder Anwendung eine eigene Chipkarte und liefert jede neue Anwendung sowie jedes Update einer bestehenden Anwendung ebenfalls eine neue Chipkarte. Grundsätzlich wünschenswert ist deshalb eine Chipkarte, die für eine Vielzahl von Anwendungen unterschiedlicher Diensteanbieter und unterschiedlicher Betreiber von Kartensystemen, wie Kreditkartenorganisationen, Banken, Versicherungen, Telefongesellschaften usw., genutzt werden kann.

Eine Dateiorganisation für eine solche für mehrere Anwendungen geeigneten Chipkarte ist aus Rankl/Effing, "Handbuch der Chipkarten", Carl Hanser Verlag, 1996, Kapitel 5.6, entnehmbar. Die darin beschriebene Organisationsstruktur beruht auf der ISO/ IEC-Norm 7816-4. An der Spitze der Dateistruktur steht dabei ein "Masterfile", das die Verzeichnisse aller anderen auf der Chipkarte vorhandenen Dateien enthält. Dem Masterfile sind ein oder mehrere "Dedicated Files" nachgeordnet, welche die Dateinamen von in Gruppen zusammengefaßten, insbesondere die zu einer Anwendung gehörenden Dateien enthalten. Jedem Dedicated File sind schließlich ein oder mehrere "Elementary Files" untergeordnet, in denen die Nutzdaten einer Anwendung liegen. Als technisch möglich, aber aus Gründen der Sicherheit nicht zweckmäßig beschreibt die Schrift desweiteren das Nachladen von Programmcode. Als vielversprechendste Maßnahme zur Überwindung der Sicherheitsbedenken verweist sie auf die Einrichtung einer "Memory Management Unit", welche auszuführenden Programmcode auf Einhaltung der zugewiesenen Grenzen überwacht.

Aus der Druckschrift WO-A1-98/09257 sind ein System und ein Verfahren zum Laden von Anwendungen auf eine Chipkarte bekannt, die es erlauben, zusätzlich zu den Daten bereits geladener Anwendungen Programm- und Anwendungsdaten weiterer Anwendungen in eine Chipkarte zu bringen. Dabei sind Vorkehrungen auf der Grundlage geeigneter kryptographischer Techniken getroffen worden, die eine Verifizierung der Befugnis der das Nachladen von Daten betreibenden Stelle gestatten. Nachdem die Daten einer zusätzlichen Anwendung in den Speicher der Chipkarte gelangt sind, wird die Authentizität der dazugehörigen Programmdaten überprüft. Sodann werden die Programmdaten hinsichtlich ihrer Syntax sowie geltender Typenbeschränkungen geprüft. Wird bei einem dieser Prüfschritte eine Unstimmigkeit festgestellt, werden die zusätzlich geladenen Daten verworfen und im Speicher gelöscht. Das bekannte System erlaubt ein kontrolliertes Nachladen von Anwendungen auch nach Ausgabe der Karte an den Endanwender. Es bedingt allerdings, daß ein Kartenausgeber, der eine Chipkarte mit verfügbarem, freiem Speicherplatz etwa an einen Diensteanbieter abgibt, selbst bereits die Identität aller Stellen des Diensteanbieters kennen muß, die später einmal berechtigt sein sollen, einem Endnutzer Anwendungen zum Nachladen anzubieten. Das kann dadurch geschehen, daß der Kartenausgeber bestimmte öffentliche Signaturschlüssel von Diensteanbietern zertifiziert, um durch Hinterlegung seines eigenen öffentlichen Signaturschlüssels, etwa in der ROM-Maske der Chipkarte, eine Überprüfung der Authentizität nachgeladener Daten leisten zu können. Ein Kartenausgeber hat bei dem bekannten System allerdings keine Möglichkeit, über die Authentizität und die syntaktische Korrektheit hinaus das von den Diensteanbietern belegte Speichervolumen auf einer einzelnen Chipkarte zu kontrollieren.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren zum Einbringen einer zusätzlichen Anwendung auf eine Chipkarte sowie eine Chipkarte anzugeben, die die genannten Nachteile des Standes der Technik vermeiden.

Diese Aufgabe wird erfindungsgemäß gelöst durch ein Verfahren mit den in Anspruch 1 angegebenen Merkmalen sowie durch eine Chipkarte mit den Merkmalen des unabhängigen Anspruchs 4. Die Aufgabe wird ebenfalls gelöst durch ein Verfahren mit den in Anspruch 8 angegebenen Merkmalen sowie durch eine Chipkarte mit den Merkmalen des unabhängigen Anspruchs 12. Die Gegenstände der Patentansprüche 1 und 4 einerseits sowie 8 und 12 andererseits haben jeweils eigenständige erfinderische Bedeutung, die Verfahren gemäß den Ansprüchen 1 und 8 sowie die Gegenstände der Ansprüche 4 und 12 lassen sich aber auch verbinden.

Das erfindungsgemäße Verfahren gemäß Anspruch 1 und ebenso das Verfahren gemäß Anspruch 8 erlauben es einem Kartenherausgeber in vorteilhafter Weise, einem Anwender das eigenmächtige, nachträgliche Einbringen von Funktionsprogrammen in eine Karte zu gestatten. Der Kartenausgeber muß nicht mehr vorab festlegen, welche Anwender oder Diensteanbieter eine Erlaubnis zum Nachladen von zusätzlichen Anwendungen auf bestimmte Chipkarten erhalten sollen. Das Nachladen einer Anwendung ist vielmehr auch dann möglich, wenn die Chipkarte bereits ausgegeben ist und sich im Besitz des Anwenders befindet. Das Verfahren eignet sich deshalb insbesondere dafür, eine vertragliche Abtretung genau umreißbarer Rechte an Speicherressourcen von Chipkarten an Dritte durch einen Chipkartenausgeber umzusetzen.

Das Verfahren gewährleistet dabei einen hohen Sicherheitsstandard. Gemäß Anspruch 1 wird er erreicht, indem zum Nachladen von Anwendungsfunktionsprogrammen befähigende Ladeapplikationen nur über eine vom Kartenherausgeber auf der Karte eingerichtete Hauptladerschnittstelle auf die Karte gebracht werden können. Mittels der Hauptladerschnittstelle lassen sich vorteilhaft insbesondere die physikalische Lage sowie der logische Wirkungsbereich eines nachgeladenen Funktionsprogrammes genau definieren. Die Schaffung einer Möglichkeit zum Nachladen von Funktionsprogrammen vereinfacht in vorteilhafter Weise zudem die Fertigung der entsprechenden Karten.

Das Ausweissystem nach Anspruch 8 bietet den Vorteil, daß der Kartenherausgeber das Volumen des Speicherplatzes kontrollieren kann, das einzelnen Anwendern für nach-

ladbare Anwendungen zur Verfügung stehen soll. Das Ausweissystem bietet desweiteren die Möglichkeit zur Einrichtung eines anwendungsbezogenen Kostensystems. Beispielsweise kann vorgesehen sein, einen Anwender oder Diensteanbieter in dem Maße an den Gesamtkosten einer Chipkarte zu beteiligen, in dem er die Speichereinrichtung der Chipkarten belegt.

Vorteilhafte Weiterbildungen und zweckmäßige Ausgestaltungen des vorgeschlagenen Verfahrens bzw. der vorgeschlagenen Chipkarte sind den abhängigen Ansprüchen entnehmbar.

Die Erfindung wird im folgenden unter Bezugnahme auf die Zeichnung anhand eines Ausführungsbeispieles exemplarisch und in nicht beschränkender Weise näher erläutert.

In der Zeichnung zeigen

Fig. 1 den strukturellen Aufbau einer Mikroprozessorchipkarte,

Fig. 2 schematisch die Belegung der Speichereinrichtung einer Chipkarte mit einem Hauptlader,

Fig. 3 die Belegung der Speichereinrichtung nach dem Laden eines Spezialladers,

Fig. 4 eine schematische Darstellung der hierarchischen Struktur aus einem Hauptlader und mehreren Spezialladern.

Fig. 1 zeigt den typischen Aufbau einer mit einem Mikroprozessor ausgerüsteten Chipkarte **10**. Hauptelement bildet eine zentrale Prozessoreinheit **20**, welche der Chipkarte **10** durch Ausführung von Funktionsprogrammen ihre Funktionalität verleiht. Der Prozessoreinheit **20** ist eine aus drei Speicherschaltungen **30**, **40**, **50** aufgebaute Speichereinrichtung **320** zugeordnet. Dabei repräsentiert die Speicherschaltung **30** einen maskenprogrammierten Nur-Lese-Speicher-Speicher (ROM), worin sich insbesondere das Betriebssystem der zentralen Prozessoreinheit **20** befindet, die Speicherschaltung **50** einen elektrisch löschbaren Nur-Lese-Speicher **50** (EEPROM) zur Aufnahme der Programmcodes von Funktionsprogrammen sowie von durch die zentrale Prozessoreinheit **20** benutzten Daten, die Speicherschaltung **40** einen, in der Regel flüchtigen, Schreib-Lese-Speicher **40** (RAM) zur Nutzung als Arbeitsspeicher bei der Ausführung eines Funktionsprogrammes. Eine Kartenfunktionalität ergibt sich aus der Gesamtheit der in den Speicherschaltungen **30**, **40**, **50** enthaltenen Programmcodes bzw. Daten. Die Speicherschaltungen **30**, **40**, **50** können dabei, falls dies technisch notwendig oder zweckmäßig ist, übergreifend genutzt werden, etwa indem bestimmte Speicheradreßbereiche im EEPROM für Programmdaten des Betriebssystems benutzt werden oder Speicheradreßbereiche im ROM mit Anwendungsdaten belegt sind. Aus diesem Grund werden die Speicherschaltungen **30**, **40**, **50** nachfolgend stets gesamtheitlich als Speichereinrichtung **110** aufgefaßt. Zum Austausch von Daten mit externen Einrichtungen besitzt die Karte **10** desweiteren eine Datenschnittstelle **60**, die ebenfalls mit der zentralen Prozessoreinheit **20** verbunden ist. Eine typische Anwendung der gezeigten Karte **10** bildet die Ausführung elektronischer Zahlungsvorgänge. Eine detaillierte Beschreibung der in **Fig.** 1 dargestellten Chipkarte findet sich im übrigen z. B. in Rankl/Effing, "Handbuch der Chipkarten", Carl Hanser Verlag, 1996, Kapitel 2.3.

Eine erste Ausgestaltung der Erfindung beruht auf dem Konzept, das Einbringen von Ladeapplikationen, welche ihrerseits Anwendungsfunktionsprogramme laden können, auf eine Karte zuzulassen, die Einrichtung der Ladeapplikationen selbst dabei aber ausschließlich einer speziellen Laderschnittstelle zu gestatten. **Fig.** 2 veranschaulicht schematisch die Belegung der Speichereinrichtung **110** einer Chipkarte, welche zunächst nur den Programmcode eines einzelnen Funktionsprogrammes **120** umfaßt, das eine erste haderschnittstelle 120 definiert. Die Laderschnittstelle **120** ist speziell dazu ausgebildet, Funktionsprogramme in die Speichereinrichtung **110** nachzuladen, die Ladeapplikationen realisieren, d. h. die ihrerseits Ladefunktionalität besitzen und das Nachladen von Anwendungsfunktionsprogrammen ermöglichen. Die Laderschnittstelle **120** bildet zweckmäßig eine Grundausstattung einer Chipkarte und wird vom Kartenherausgeber oder Kartenhersteller auf die Karte gebracht. Die im folgenden als Hauptlader (HL) bezeichnete Laderschnittstelle **120** belegt einen Teil des gesamten in der Speichereinrichtung **110** zur Verfügung stehenden Speicherbereiches. Ein anderer Teil des Gesamtspeicherbereiches ist zunächst nicht mit Daten belegt und steht als Freispeicher **130** für noch zu ladende weitere Funktionsprogramme zur Verfügung. Die Verwaltung des gesamten Freispeichers **130** erfolgt zunächst durch den Hauptlader **120**. Er steuert insbesondere das Laden des Programmcodes des ersten nachzuladenden Funktionsprogrammes in den Freispeicher **130**. Der Bytecode des ersten wie auch aller weiteren nachgeladenen Funktionsprogramme wird in Form geeigneter elektrischer Signale über die Datenschnittstelle **60** übermittelt.

Der Hauptlader **120** lädt bevorzugt nur solche Funktionsprogramme in die Speichereinrichtung **110**, die definierte Sicherheitsvoraussetzungen erfüllen. Beim Laden prüft er dazu vorzugsweise Integrität und Authentizität einer zu ladenden Ladeapplikation durch Prüfung, ob der zum Laden anstehende Programmcode unverändert in einer vom Hersteller gebilligten Form vorliegt, oder ob der Hersteller einer Ladeapplikation tatsächlich zum Einbringen der Ladeapplikation befugt ist, indem er zum Beispiel vom Kartenausgeber ein Recht zur Nutzung von Chipkarten-Ressourcen erworben hat.

Fig. 3 zeigt die Speicheranordnung aus **Fig.** 2, wobei der Hauptlader **120** jetzt ein erstes, eine Ladeapplikation realisierendes Funktionsprogramm **210** in den Freispeicher **130** geladen hat. Die Ladeapplikation **210** definiert eine zweite, im folgenden als Speziallader **210** (DL) bezeichnete Schnittstelle. Sie erlaubt es, nachfolgend weitere Funktionsprogramme in die Speichereinrichtung **110** zu bringen. Dafür steht ihr jedoch nur ein definierter, nicht erweiterbarer Verfügungsadreßraum **220** bereit. Der Verfügungsadreßraum **220** wird dem Speziallader **210** vom Hauptlader **120** beim Laden des Spezialladers **210** zugeteilt. Mit Zuteilung geht dabei die Verwaltung des Verfügungsadreßraumes **220** vollständig an den Speziallader **210** über. Der Hauptlader **120** hat auf die weitere Nutzung des dem Speziallader **210** zugeordneten Verfügungsadreßraumes **220** keinen Einfluß und keine Zugriffsmöglichkeit mehr. Weiterhin unter Verwaltung des Hauptladers verbleibt der noch nicht belegte, durch Übernahme des Spezialladers **210** und Zuteilung des Verfügungsadreßraumes **220** in separate Abschnitte **130a**, **130b** fragmentierte Teil des Freispeicheradreßraumes.

Das Laden eines Spezialladers **210** kann, im Unterschied zum Hauptlader **120**, durch den Anwender einer Karte erfolgen. Der Speziallader **210** ermöglicht es und ist Voraussetzung dafür, daß der Anwender nachfolgend Anwendungen realisierende Funktionsprogramme nach eigener Wahl in den Verfügungsadreßraum **220** laden kann. Bei der Übernahme neuer Funktionsprogramme in den Verfügungsadreßraum **220** stellt der Speziallader **210** sicher, daß der Programmcode eines geladenen Funktionsprogrammes keinesfalls auf außerhalb des Verfügungsadreßraumes **220** liegenden Datencode zugreifen kann. Der einem Speziallader **210** zugeteilte Verfügungsadreßraum **220** kann dabei schon beim Laden durch den Hauptlader **120** mit Sicherungen versehen worden sein, die einen physikalischen oder logischen Zugriff auf außerhalb des Verfügungsadreßraumes **220** liegende Teilbereiche der Speichereinrichtung **110** verhindern. Die Aufteilung des Verfügungsadreßraumes **220** auf nach-

geladene Funktionsprogramme erfolgt durch den Speziallader **210**. Einem Funktionsprogramm **230** zur Realisierung einer neuen Kartenanwendung kann dabei beispielsweise ein Teilbereich **231** des Verfügungsadreßraumes **220** zugewiesen worden sein.

In einer besonders für eine Überlassung von Speicherbereich an Dritte günstigen Ausprägung der vorstehend beschriebenen Struktur ist die Belegung der Speichereinrichtung **110**, wie in **Fig. 4** gezeigt, hierarchisch strukturiert. Die angedeutete Baumstruktur veranschaulicht dabei die zeitliche Abfolge des Einbringens der unterschiedlichen Funktionsprogramme. Im Minimalzustand ist die Karte nur mit einem Hauptlader **120** ausgestattet, er bildet zunächst den einzigen Zugang zur Speichereinrichtung **110** der Karte. Der Hauptlader **120** ermöglicht das Laden von Spezialladern **210a**, **210b**, **210c** sowie von allgemeinen Funktionen bzw. Kartengrundfunktionen realisierenden Funktionsprogrammen **240**. Befindet sich ein Hauptlader **120** auf einer Karte, können Speziallader **210** und Funktionsprogramme **240** zu beliebigen Zeitpunkten über den Hauptlader **120** geladen werden, sie sind in der Baumstruktur der **Fig. 3** daher als vom Hauptlader ausgehende, parallele Pfade dargestellt.

Alle neu geladenen Funktionsprogramme **120**, **240** werden beim Laden durch den Hauptlader **120** auf Zulässigkeit und Sicherheit geprüft. Nur positiv geprüfte Funktionsprogramme werden geladen. Geladenen Spezialladern **210a**, b, c teilt der Hauptlader **120** in der Speichereinrichtung **110** jeweils einen unverrückbar lagedefinierten, durch den zugehörigen Speziallader **210** nicht erweiterbaren Verfügungsadreßraum **220** zu. Das den Speziallader **210** realisierende Funktionsprogramm kann dabei Informationen zur Größe des benötigten Verfügungsadreßraumes **220** enthalten. Erhält der Hauptlader **120** keine Größeninformationen, teilt er einen Standardverfügungsadreßraum zu. Beim Laden von Funktionsprogrammen **210**, **240** stellt der Hauptlader **120** sicher, daß die Verfügungsadreßräume **220** verschiedener Speziallader **210** logisch und physikalisch streng getrennt sind und ein Zugriff eines Spezialladers **210** auf den Verfügungsadreßraum **220** eines anderen Spezialladers **210** nicht möglich ist. Nach Laden und Verfügungsadreßraumzuteilung geht die Kontrolle über den jeweiligen Verfügungsadreßraum **220** jeweils vollständig und ausschließlich auf den zugehörigen Speziallader **210a**, **210b**, **210c** über.

Jeder Speziallader **210** kann nun in den jeweils zugeteilten Verfügungsadreßraum **220** weitere Funktionsprogramme laden, insbesondere Funktionsprogramme, die Kartenanwendungen realisieren, etwa kryptographische Schlüssel oder Verfahren zu sicheren Durchführung von Finanztransaktionen. Den zu einem zu ladenden Funktionsprogramm gehörenden Bytecode unterwirft der Speziallader **210** beim Laden einer Sicherheits- und Zulässigkeitsprüfung. Desweiteren legt der Speziallader **210** beim Laden eines Funktionsprogrammes dessen mögliche Zugriffsrechte und Verbindungsmöglichkeiten in Bezug auf andere, in der Speichereinrichtung **110** bereits vorhandene Funktionsprogramme fest. Dabei kann er insbesondere auch Beschränkungen einrichten, welche beispielsweise den Zugriff auf oder die Verbindung eines neugeladenen Funktionsprogrammes mit einem bereits vorhandenen oder noch nachladbaren Funktionsprogramm verhindern.

Im Ausführungsbeispiel der **Fig. 4** haben der Speziallader **210a** zwei Funktionsprogramme **310**, **311**, der Speziallader **210b** drei Funktionsprogramme **320**, **321**, **322**, der Speziallader **210c** ein weiteres Funktionsprogramm **330** geprüft, zugelassen und in den jeweils zugeteilten Verfügungsadreßraum **220** geladen. Das Nachladen der Funktionsprogramme **310**, **311**, **320**, **321**, **322**, **330** kann, wenn der benötigte Speziallader **210** auf der Karte vorhanden ist, durch den Speziallader **210** zu beliebigen Zeitpunkten und in beliebiger Reihenfolge geschehen. In **Fig. 4** ist jedes nachgeladene Funktionsprogramm **310**, **311**, **320**, **321**, **322**, **330** entsprechend dem jeweils ladenden Speziallader **210a**, **210b** bzw. **210c** zugeordnet. Die Funktionsprogramme **310**, **311**, **320**, **321**, **322**, **330** können, wenn das beim Laden durch die jeweils eingeschalteten Speziallader **210** zugelassen wurde, aufeinander zugreifen oder miteinander verbunden werden. Im Beispiel der **Fig. 4** kann etwa das Funktionsprogramm **330** auf die Funktionsprogramme **321** oder **310** zugreifen, um etwa darin angelegte Prozeduren selbst zu verwenden. Keine Zugriffs- oder Verbindungsmöglichkeit hat das Funktionsprogramm **330** andererseits bezüglich der Funktionsprogramme **311**, dieses ist speziell für das Funktionsprogramm **330** gesperrt oder 320, dieses ist für alle Fremdzugriffe gesperrt.

Komplementär zum Laden neuer Funktionsprogramme durch den Hauptlader **120** oder einen Speziallader **210** ist grundsätzlich auch das Löschen von in einer Speichereinrichtung **110** vorhandenen Funktionsprogrammen **120**, **240**, **310**, **330** möglich. Die Berechtigung zum Löschen wird jeweils beim Laden eines Funktionsprogrammes durch den Lader **120**, **210** eingerichtet. Das Löschen eines Speziallladers **210** ist nur möglich, wenn sich in dem ihm zugeteilten Verfügungsadreßraum **220** kein Funktionsprogramm mehr befindet. Der Hauptlader **120** kann nicht gelöscht werden.

Eine Maßnahme, welche eine risikoarme Überlassung von Chipkartenspeicherraum an Dritte vorteilhaft unterstützt, ist die Nutzung eines Ausweissystems für die Durchführung der Speicherraumzuteilung durch Hauptlader **120** und/oder Speziallader **210a**, **210b**, **210c**. Die Ausweise haben dabei die Gestalt einer digitalen Information. Sie werden einem zu ladenden Funktionsprogramm **210** beigegeben und beinhalten insbesondere eine Angabe über die Größe des gewünschten Verfügungsadreßraumes **220**. Der Lader **120**, **210**, über den ein mit einem Ausweis versehenes Funktionsprogramm geladen werden soll, muß zur Auswertung des Ausweises fähig sein. Ein Ausweissystem kann für alle Lader **120**, **210** einer Karte oder auch nur für einzelne eingerichtet sein; eine hierarchische Laderstruktur wie in **Fig. 3** gezeigt ist keine Voraussetzung für seine Einrichtung. Die Ausweise werden vom Chipkartenherausgeber oder dem Hersteller eines Laders **120**, **210** generiert. Von jenem müssen sie auch für ein neu in eine Speichereinrichtung **110** zu ladendes Funktionsprogramm vorab erworben werden. Der Laderhersteller/Kartenherausgeber ist auf diese Weise stets über die Belegung des seinem Lader **120/210** zugeordneten Verfügungsadreßraumes informiert. Indem er neu zu ladenden Funktionsprogrammen nur den unbedingt notwenigen Adreßraum zuweist, kann er dabei mittels einer entsprechenden Information auf dem Ausweis eine besonders speicherplatzssparende Nutzung eines zugeteilten Verfügungsadreßraumes sicherstellen.

Neben einer reinen Größeninformation kann ein Ausweis weitere Informationen enthalten, etwa Informationen, welche die Prüfung der Authentizität eines Ausweises ermöglichen. Echtheit und Fälschungssicherheit eines Ausweises werden weiter vorzugsweise durch kryptographische Verfahren gewährleistet. Die Informationen auf einem Ausweis sind hierbei verschlüsselt, der Ausweis enthält entsprechend beispielsweise einen Initialisierungsschlüssel, welcher es einem autorisierten Lader erlaubt, einen Schlüssel zum Lesen des Ausweises abzuleiten. Zweckmäßig enthält ein Ausweis ferner eine kryptographisch realisierte digitale Signatur. Zur Erleichterung der Verwaltung können auf einem Ausweis desweiteren beispielsweise die Bezeichnung eines Funktionsprogrammes, eine Anwendungskennung, ein Datum, o. ä. angelegt sein. Möglich ist weiterhin die Einrichtung

von Informationen, welche die Nutzbarkeit eines Funktionsprogrammes beschränken; beispielsweise kann die zeitliche Nutzbarkeit einer Anwendung beschränkt werden, oder es können Kennungen von Karten angegeben sein, welche alleine zur Nutzung eines Funktionsprogrammes berechtigt sind.

Patentansprüche

1. Verfahren zum Betreiben eines mit einer Datenübertragungseinrichtung, einer Speichereinrichtung sowie einer Programmausführungseinheit zur Ausführung von in der Speichereinrichtung enthaltenen Funktionsprogrammen ausgestatteten Datenträgers mit folgenden Schritten:
   - Installieren eines eine Laderschnittstelle (**120**) zum Nachladen weiterer Ladeapplikationen (**210**) realisierenden Funktionsprogrammes in der Speichereinrichtung (**110**) des Datenträgers,
   - Bereitstellen eines verfügbaren Freispeicherraumes (**130**) in der Speichereinrichtung (**110**) für die Laderschnittstelle,
   - Nachladen mindestens einer Ladeapplikation (**210**) über die Datenübertragungseinrichtung (**60**) in die Speichereinrichtung (**110**) unter Kontrolle der Laderschnittstelle, wobei der Ladeapplikation (**210**) ein Teil des Freispeicherraums (**130**) als Verfügungsadreßraum (**220**) zugeteilt wird.

2. Verfahren nach Anspruch 1, gekennzeichnet durch folgenden weiteren Schritt:
Nachladen mindestens eines Anwendungsprogrammes (**230**) über die Datenübertragungseinrichtung (**60**) durch die Programmausführungseinheit unter der Kontrolle der Ladeapplikation (**210**) in den dieser zugeteilten Verfügungsadreßraum (**220**).

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Laderschnittstelle (**120**) die Kontrolle über einen einer Ladeapplikation (**210**) zugewiesenen Verfügungsadreßraum (**220**) an die Ladeapplikation (**210**) abgibt.

4. Datenträger mit
   - einer Speichereinrichtung (**110**) zur Aufnahme von Funktions- und Anwendungsprogrammen, einer Programmausführungseinheit (**20**) zur Ausführung von in der Speichereinrichtung (**110**) enthaltenen Funktionsprogrammen,
   - einer Datenübertragungseinrichtung (**60**),
   - sowie einer als Funktionsprogramm realisierten Laderschnittstelle (**120**) zum Laden von mindestens einer das Nachladen eines weiteren Anwendungsprogrammes ermöglichenden Ladeapplikation (**210**) in die Speichereinrichtung (**110**) über die Datenübertragungseinrichtung (**60**),
   - wobei der Laderschnittstelle (**120**) in der Speichereinrichtung (**110**) ein Freispeicherraum (**130**) zur Aufnahme mindestens einer Ladeapplikation zugeordnet ist.

5. Datenträger nach Anspruch 4, dadurch gekennzeichnet, daß eine in die Speichereinrichtung (**110**) aufgenommene Ladeapplikation (**210**) unabhängig von der Laderschnittstelle (**120**) einen Teil (**220**) des der Laderschnittstelle zugeordneten Freispeicherraums (**130**) kontrolliert.

6. Datenträger nach Anspruch 4, dadurch gekennzeichnet, daß die Ladeapplikationen (**210**) dazu ausgebildet sind, nachzuladene Anwendungsprogramme (**330**) während des Ladens mit auf dem Datenträger bereits vorhandenen Anwendungs- und Funktionsprogrammen zu verbinden.

7. Datenträger nach Anspruch 6, dadurch gekennzeichnet, daE eine Ladeapplikation (**210**) Beschränkungen beinhaltet, welche die Verbindung eines neuzuladenden Anwendungsprogrammes (**330**) mit einem bereits vorhandenen (**311, 320**) verbieten.

8. Verfahren zum Betreiben eines eine Speichereinrichtung zur Aufnahme von Funktions- und Anwendungsprogrammen, eine Programmausführungseinheit zur Ausführung von in der Speichereinrichtung enthaltenen Funktions- und Anwendungsprogrammen, sowie eine Datenübertragungseinrichtung aufweisenden Datenträgers mit folgenden Schritten:
   - Ausrüsten des Datenträgers mit einem eine Laderschnittstelle (**120, 210**) realisierenden Funktionsprogramm zum Nachladen von Anwendungsprogrammen in die Speichereinrichtung,
   - Ausrüsten des Datenträgers mit einer Verwaltungseinrichtung zum Zuteilen von Adreßräumen in der Speichereinrichtung (**110**) an nachgeladene Anwendungsprogramme,
   - Versehen der nachzuladenen Anwendungsprogramme mit Ausweisen, welche eine Information über die Größe des für das Anwendungsprogramm benötigten Speicherplatzes enthalten,
   - Auswerten des Ausweises beim Nachladen eines Anwendungsprogrammes, und
   - Zuteilen eines auf die ermittelte Größeninformation abgestimmten Adreßraumes in der Speichereinrichtung (**110**) an das Anwendungsprogramm.

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß der Ausweis weiterhin eine das Anwendungsprogramm bezeichnende Information enthält.

10. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß der Ausweis weiterhin eine Signatur zum Nachweis der Echtheit des Anwendungsprogrammes enthält.

11. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß die Ausweise vom Herausgeber des Datenträgers ausgegeben werden.

12. Datenträger mit einer Speichereinrichtung (**110**) zur Aufnahme von Funktions- und Anwendungsprogrammen, einer Programmausführungseinheit (**20**) zur Ausführung von in der Speichereinrichtung enthaltenen Funktionsprogrammen, einer Datenübertragungseinrichtung (**60**), sowie einer als Funktionsprogramm realisierten Laderschnittstelle (**120, 210**) zum Nachladen von mindestens einem Anwendungsprogramm in die Speichereinrichtung über die Datenübertragungseinrichtung (**60**), wobei die Laderschnittstelle (**120, 210**) Mittel zum Prüfen eines Ausweises eines zu ladenden Anwendungsprogrammes aufweist und sie einem zu ladenden Anwendungsprogramm entsprechend einer auf dem Ausweis enthaltenen Größeninformation Speicherplatz in der Speichereinrichtung (**110**) zuteilt.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 199 29 164 A1
Int. Cl.[7]: G 07 F 7/10
Offenlegungstag: 11. Januar 2001

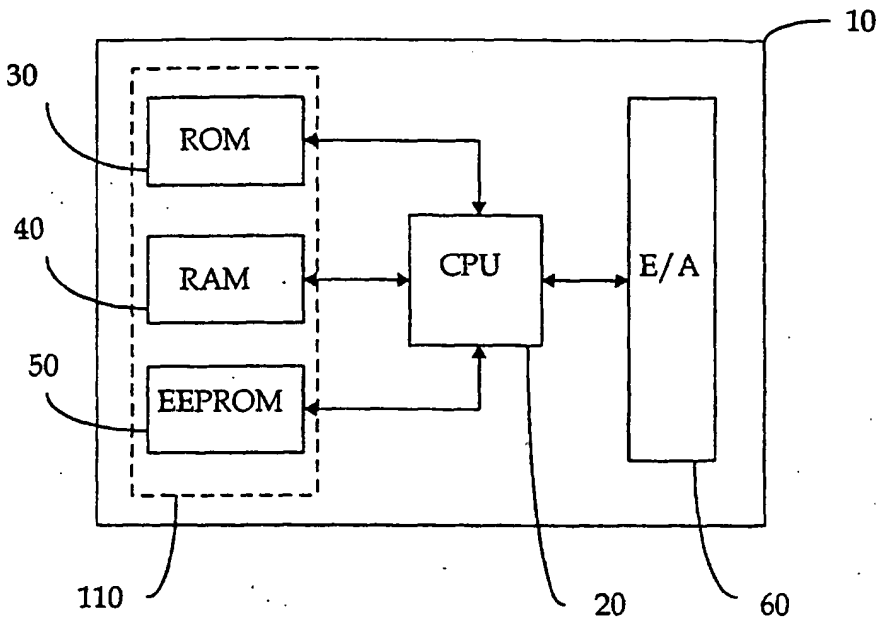

Fig. 1

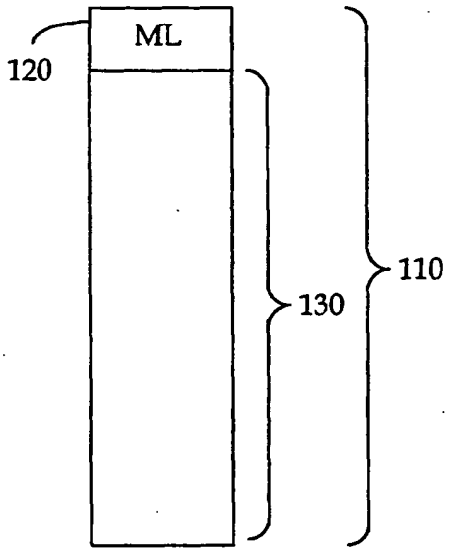

Fig. 2

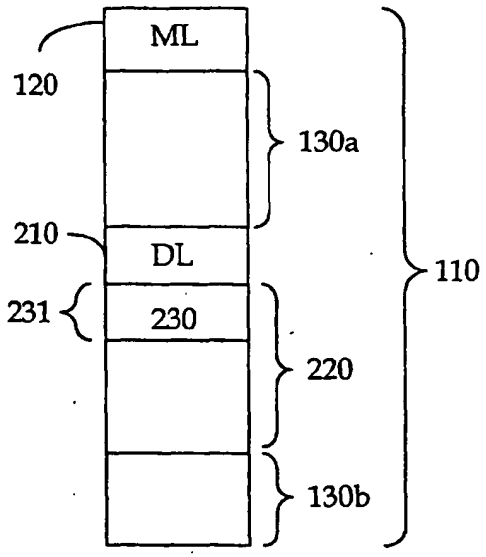

Fig. 3

Nummer: DE 199 29 164 A1
Int. Cl.[7]: G 07 F 7/10
Offenlegungstag: 11. Januar 2001

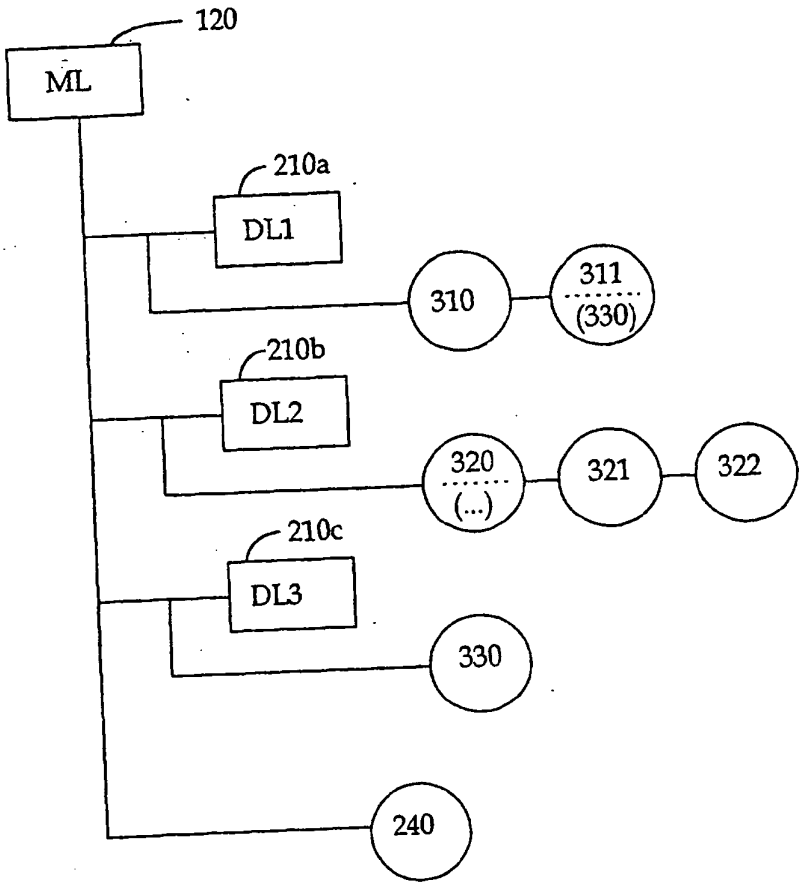

Fig. 4